United States General Accounting Office

GAO

Testimony

Before the Subcommittees on Cybersecurity, Science, and Research & Development and Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:30 a.m. EDT
Wednesday, April 21, 2004

CRITICAL INFRASTRUCTURE PROTECTION

Establishing Effective Information Sharing with Infrastructure Sectors

Statement of Robert F. Dacey
Director, Information Security Issues

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-699T, testimony before the Subcommittees on Cybersecurity, Science, and Research & Development and on Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Critical infrastructure protection (CIP) activities that are called for in federal policy and law are intended to enhance the security of the cyber and physical public and private infrastructures that are essential to our nation's security, economic security, or public health and safety. As reliance on these infrastructures increases, so do the potential threats and attacks that could disrupt critical systems and operations. Effective information-sharing partnerships between industry sectors and government can contribute to CIP efforts.

Federal policy has encouraged the voluntary creation of information sharing and analysis centers (ISACs) to facilitate the private sector's participation in CIP by serving as mechanisms for gathering and analyzing information and sharing it among the infrastructure sectors and between the private sector and government. This testimony discusses the management and operational structures used by ISACs, federal efforts to interact with and support the ISACs, and challenges to and successful practices for ISACs' establishment, operation, and partnerships with the federal government.

www.gao.gov/cgi-bin/getrpt?GAO-04-699T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at 202-512-3317 or Daceyr@gao.gov.

CRITICAL INFRASTRUCTURE PROTECTION

Establishing Effective Information Sharing with Infrastructure Sectors

What GAO Found

Federal awareness of the importance of securing the nation's critical infrastructures—and the federal government's strategy to encourage cooperative efforts among state and local governments and the private sector to protect these infrastructures—have been evolving since the mid-1990s. Federal policy continues to emphasize the importance of the ISACs and their information-sharing functions. In addition, federal policy established specific responsibilities for the Department of Homeland Security (DHS) and other federal agencies involved with the private sector in CIP. The ISACs themselves, although they have similar missions, were developed to serve the unique needs of the sectors they represent, and they operate under different business models and funding mechanisms.

According to ISAC representatives and a council that represents many of them, a number of challenges to their successful establishment, operation, and partnership with DHS and other federal agencies remain. These challenges include increasing the percentage of entities within each sector that are members of its ISAC; building trusted relationships and processes to facilitate information sharing; overcoming barriers to information sharing; clarifying the roles and responsibilities of the various government and private sector entities that are involved in protecting critical infrastructures; and funding ISAC operations and activities. According to a DHS official, these issues are being considered, and the department is developing a plan that will document the current information-sharing relationships among DHS, the ISACs, and other agencies; goals for improving those information-sharing relationships; and methods for measuring progress toward these goals.

Information Sharing and Analysis Centers by Sector

Sector	ISAC	Established
Banking and Finance	Financial Services	October 1999
Chemicals & Hazardous Materials	Chemical	April 2002
Emergency Services	Emergency Management & Response	October 2000
Energy	Electric	October 2000
Energy	Energy	November 2001
Food	Food	February 2002
Government	Multi-State	January 2003
Information Technology & Telecommunications	IT	December 2000
	Telecom	January 2000
	Research & Education Network	February 2003
Transportation	Public Transit	January 2003
	Surface Transportation	May 2002
	Highway	March 2003
Drinking Water & Water Treatment Systems	Water	December 2002
Other	Real Estate	April 2003

Source: GAO

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to discuss the status of private-sector information sharing and analysis centers (ISACs) and their efforts to help protect our nation's critical infrastructures. Critical infrastructure protection (CIP) activities called for in federal policy and law are intended to enhance the security of cyber and physical, public and private infrastructures that are essential to national security, national economic security, or national public health and safety. Beginning with Presidential Decision Directive 63 (PDD 63) issued in May 1998, federal policy has encouraged the voluntary creation of ISACs to facilitate private-sector participation and serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government. Subsequent federal CIP policy, including several national strategies, continued to emphasize the importance of the ISACs and their information-sharing functions.[1] Further, CIP policy has established specific responsibilities for the Department of Homeland Security (DHS) and other federal agencies with respect to public-private collaboration to help protect private infrastructure sectors.

In my testimony today, I will discuss the management and operational structures used by the ISACs, including their estimated sector participation, business and funding models, and information sharing and analysis mechanisms. I will then discuss activities by DHS and other federal agencies with responsibilities for specific infrastructure sectors to interact and support the ISACs. Lastly, I will discuss some of the ISAC-identified challenges to and successful practices for their establishment, operation, and partnership with the federal government.

As agreed, this testimony includes initial results of our ongoing analysis of private-sector ISACs, which was requested by your subcommittees. In conducting this work, we contacted officials for the 15 different ISAC organizations that had been established at the time of our review: Chemical, Electricity, Energy, Emergency Management and Response, Financial Services, Food, Information Technology, Multi-State, Public Transit, Real Estate, Research and Education, Surface Transportation, Telecommunications, Highway, and Water. Through structured interviews

[1]The White House, The National Strategy to Secure Cyberspace (Washington, D.C.: February 2003); The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Washington, D.C.: February 2003); and Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection (Washington, D.C.: Dec. 17, 2003).

with these officials, we obtained and analyzed information to describe the ISACs' current organization and operational models, funding mechanisms, sector representation and membership criteria, as well as their challenges and successful practices in establishing effective information-sharing relationships within their sectors and with the federal government. We also contacted officials of the Healthcare Sector Coordinating Council to discuss their efforts to establish an ISAC for the healthcare sector. Further, we contacted officials of the ISAC Council, which was created by 11 ISACs to address common issues, and obtained and analyzed its series of white papers on a range of ISAC-related issues and challenges. Within the federal government, we obtained and analyzed information on efforts to work with the private-sector by DHS and other agencies assigned responsibilities for specific industry sectors, including the Departments of Agriculture, Energy, Health and Human Services, and the Treasury and the Environmental Protection Agency. We did not validate the accuracy of the data provided by the ISACs, DHS, or other agencies. We performed our work from November 2003 to April 2004, in accordance with generally accepted government auditing standards.

Results in Brief

Beginning with PDD 63, federal policy has encouraged the voluntary creation of ISACs as key information-sharing mechanisms between the federal government and critical infrastructures. While PDD 63 suggested certain ISAC activities, CIP policy has essentially left the actual design and function of the ISACs to the entities that formed them. As a result, although their overall missions are similar, the current ISACs were established and developed based on the unique characteristics and needs of their individual sectors. They operate under different management and operational structures and, among other things, have different business models and funding mechanisms. For example, most are managed or operated as private entities with some, such as the Water and Chemical ISACs, part of associations that represent their sectors. Others have partnered with government agencies, such as the Telecommunications ISAC, which is a government-industry operational and collaborative body sponsored by DHS's National Communications Systems/ National Coordinating Center (NCC). Different funding mechanisms used by the ISACs include fee-for-service, association sponsorship, federal grants, and/or voluntary or in-kind operations by ISAC participants. Examples of fee-for-service funding include the Financial Services, Information Technology, and Water ISACs that offer tiered memberships with fees based on the level of service provided.

DHS and the sector-specific agencies have undertaken a number of efforts to address the public-private partnership called for by federal CIP policy and continue to work on their cooperation and interaction with the ISACs

and with each other. For example, in January 2004, DHS held a 2-day conference to describe the information they are analyzing and its use in the partnership with the private sector and to discuss information sharing between the federal government and the private sector. Also, in February, the department established the Protected Critical Infrastructure Information (PCII) Program that enables the private sector to voluntarily submit infrastructure information to the government, which can be protected from disclosure according to provisions of the Critical Infrastructure Information Act of 2002.

According to ISAC representatives and a council that represents many of them, a number of challenges remain to their successful establishment, operation, and partnership with DHS and other federal agencies. These challenges include increasing the percentage of sector entities that are members of the ISACs; building trusted relationships and processes to facilitate information sharing; overcoming barriers to information sharing, including the sensitivity of the information, legal limits on disclosure (such as Privacy Act limitations on disclosure of personally identifiable information), and contractual and business limits on how and when information is disclosed; clarifying the roles and responsibilities of the various government and private sector entities involved in protecting the critical infrastructures; and funding ISAC operations and activities. According to a DHS official, these issues are being considered and should be clarified through the department's development of a plan that documents the current information-sharing relationships between DHS, the ISACs, and other agencies; goals for improving that information-sharing relationship; and methods for measuring progress.

Background

As reliance on our nation's critical infrastructures grows, so do the potential threats and attacks that could disrupt critical systems and operations. In response to the potential consequences, federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990s. For example, issued in 1998, Presidential Decision Directive 63 (PDD 63) described the federal government's strategy for cooperative efforts with state and local governments and the private-sector to protect the systems that are essential to the minimum operations of the economy and the government from physical and cyber attack. In 2002, the Homeland Security Act created the Department of Homeland Security, which was given responsibility for developing a national plan; recommending measures to protect the critical infrastructure; and collecting, analyzing, and disseminating information to government and private-sector entities to deter, prevent and respond to terrorist attacks.

More recently, issued in December 2003, HSPD-7 defined federal responsibilities for critical infrastructure protection, superseding PDD 63.

CIP Policy Has Continued to Evolve

Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Over the years, a variety of working groups has been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. Key documents that have shaped the development of the federal government's CIP policy include:

- Presidential Decision Directive 63 (PDD 63),
- The Homeland Security Act of 2002,
- The *National Strategies for Homeland Security*, to *Secure Cyberspace* and *for the Physical Protection of Critical Infrastructures and Key Assets*, and
- Homeland Security Presidential Directives 7 (HSPD-7) and 9 (HSPD-9).

Presidential Decision Directive 63 Established an Initial CIP Strategy

In 1998, the President issued PDD 63, which described a strategy for cooperative efforts by government and the private-sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions that were intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private-sector. Although superseded in December 2003 by HSPD-7, PDD 63 provided the foundation for the development of the current sector-based CIP approach.

To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support, including the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response.

To ensure the coverage of critical sectors, PDD 63 identified eight infrastructures and five functions. For each of the infrastructures and functions, the directive designated lead federal agencies, referred to as sector liaisons, to work with their counterparts in the private-sector, referred to as sector coordinators. Among other responsibilities, PDD 63 stated that sector liaisons should identify and access economic incentives to encourage sector information sharing and other desired behavior.

To facilitate private-sector participation, PDD 63 also encouraged the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. PDD 63 also suggested several key ISAC activities to effectively gather, analyze, and disseminate information—activities that could improve the security postures of the individual sectors and provide an improved level of communication within and across sectors and all levels of government. These activities are: establishing baseline statistics and patterns on the various infrastructures; serving as a clearinghouse for information within and among the various sectors; providing a library of historical data for use by the private-sector and government, and reporting private-sector incidents to NIPC.

The Homeland Security Act of 2002 Established the Department's CIP Responsibilities

The Homeland Security Act of 2002, signed by the President on November 25, 2002, established DHS. To help accomplish its mission, the act established five under secretaries, among other entities, with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security**,** and emergency preparedness and response.

The act made the Information Analysis and Infrastructure Protection (IAIP) Directorate within the department responsible for CIP functions and transferred to it the functions, personnel, assets, and liabilities of several existing organizations with CIP responsibilities, including NIPC (other than the Computer Investigations and Operations Section).

IAIP is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other threat and incident information from respective agencies of federal, state, and local governments and the private-sector, and for combining and analyzing such information to identify and assess the nature and scope of terrorist threats. IAIP is also tasked with coordinating with other federal agencies to administer the Homeland Security Advisory System to provide specific warning information along with advice on appropriate protective measures and countermeasures. Further, IAIP is responsible for disseminating, as appropriate, information analyzed by DHS within the department, to other federal agencies, to state and local government agencies, and to private-sector entities.

Moreover, as stated in the Homeland Security Act of 2002, IAIP is responsible for (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States and (2) recommending measures to protect the key resources and critical

infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private-sector, and other entities.

National Strategies Establish Information-Sharing Initiatives

The *National Strategy for Homeland Security* identifies information sharing and systems as one foundation for evaluating homeland security investments across the federal government. It also identifies initiatives to enable critical infrastructure information sharing and to integrate sharing across state and local government, private industry, and citizens. Consistent with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use all available policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation.

The *National Strategy to Secure Cyberspace* provides an initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It also provides direction to federal departments and agencies that have roles in cyberspace security and identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The strategy warns that the nation's private-sector networks are increasingly targeted and will likely be the first organizations to detect attacks with potential national significance. According to the cyberspace strategy, ISACs, which possess unique operational insight into their industries' core functions and will help provide the necessary analysis to support national efforts, are expected to play an increasingly important role in the National Cyberspace Security Response System[2] and the overall missions of homeland security. In addition, the cyberspace strategy identifies DHS as the central coordinator for cyberspace efforts and requires it to work closely with the ISACs to ensure that they receive timely and threat and vulnerability data that can be acted on and to coordinate voluntary contingency planning efforts. The strategy reemphasizes that the federal government encourages the private-sector to continue to establish ISACs and, further, to enhance the analytical capabilities of existing ISACs. Moreover, the strategy

[2]The National Cyberspace Security Response System is a public-private architecture, coordinated by the Department of Homeland Security, for analyzing and warning; managing incidents of national significance; promoting continuity in government systems and private-sector infrastructures; and increasing information sharing across and between organizations to improve cyberspace security. It includes governmental entities and nongovernmental entities, such as private-sector ISACs.

stresses the need to improve and enhance public-private information sharing about cyber attacks, threats, and vulnerabilities and to encourage broader information sharing on cybersecurity among nongovernmental organizations with significant computing resources. *The National Strategy to Secure Cyberspace* also states that the market is to provide the major impetus to improve cybersecurity and that regulation will not become a primary means of securing cyberspace.

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks. It outlines three key objectives to focus the national protection effort: (1) identifying and assuring the protection of the most critical assets, systems, and functions; (2) assuring the protection of infrastructures that face an imminent threat; and (3) pursuing collaborative measures and initiatives to assure the protection of other potential targets. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* also states that further government leadership and intense collaboration between public- and private-sector stakeholders is needed to create a more effective and efficient information-sharing process to enable our core protective missions. Some of the specific initiatives include

- defining protection-related information requirements and establishing effective, efficient information-sharing processes;
- promoting the development and operation of critical sector ISACs, including developing advanced analytical capabilities;
- improving processes for domestic threat data collection, analysis, and dissemination to state and local governments and private industry; and
- completing implementation of the Homeland Security Advisory System.

The *National Strategy for the Protection of Critical Infrastructures and Key Assets* reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets.

Current Federal Agency CIP Responsibilities

In December 2003, the President issued HSPD-7, which established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attack. It superseded PDD 63. HSPD-7 defines

responsibilities for DHS, lead federal agencies, or sector-specific agencies that are responsible for addressing specific critical infrastructure sectors, and other departments and agencies. It instructs federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks.

The Secretary of Homeland Security is assigned several responsibilities, including

- coordinating the national effort to enhance critical infrastructure protection;
- identifying, prioritizing, and coordinating the protection of critical infrastructure, emphasizing protection against catastrophic health effects or mass casualties;
- establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors; and
- serving as the focal point for cyberspace security activities, including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for critical infrastructure information systems.

To ensure the coverage of critical sectors, HSPD-7 designated sector-specific agencies, formerly referred to as lead agencies, for the critical infrastructure sectors identified in the *National Strategy for Homeland Security* (see table 1). These agencies are responsible for infrastructure protection activities in their assigned sectors, which include

- coordinating and collaborating with relevant federal agencies, state and local governments, and the private-sector to carry out their responsibilities;
- conducting or facilitating vulnerability assessments of the sector;
- encouraging the use of risk management strategies to protect against and mitigate the effects of attacks against the critical infrastructure.
- identifying, prioritizing, and coordinating the protection of critical infrastructure;

- facilitating the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices; and

- reporting to DHS on an annual basis on their activities to meet these responsibilities.

Further, the sector-specific agencies are to continue to encourage the development of information-sharing and analysis mechanisms and to support sector-coordinating mechanisms. HSPD-7 does not suggest any specific ISAC activities.

Table 1: Critical Infrastructure Sectors Identified by the *National Strategy for Homeland Security* and HSPD-7

Sector	Description	Sector-specific agency
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and Finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry represents a $450 billion enterprise and produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction and other necessities.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security

Sector	Description	Sector-specific agency
Public Health and Healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security
Drinking water and water treatment systems	Sanitizes the water supply with the use of about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency

Source: GAO analysis based on the President's National Strategy documents and HSPD-7.

In January, the President issued HSPD-9, which established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. HSPD-9 defines responsibilities for DHS, lead federal agencies, or sector-specific agencies, responsible for addressing specific critical infrastructure sectors, and other departments and agencies. It instructs federal departments and agencies to protect the agriculture and food system from terrorist attacks, major disasters, and other emergencies by

- identifying and prioritizing sector-critical infrastructure and key resources for establishing protection requirements;
- developing awareness and early warning capabilities to recognize threats;
- mitigating vulnerabilities at critical production and processing nodes;
- enhancing screening procedures for domestic and imported products; and
- enhancing response and recovery procedures.

In addition, the Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, and other appropriate federal department and agencies, are assigned responsibilities including:

- expanding and continuing vulnerability assessments of the agriculture and food sectors; and
- working with appropriate private-sector entities to establish an effective information-sharing and analysis mechanism for agriculture and food.

Prior GAO Recommendations

We have made numerous recommendations over the last several years related to information-sharing functions that have been transferred to DHS. One significant area of our work concerns the federal government's CIP efforts, which is focused on sharing information on incidents, threats, and vulnerabilities and providing warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private-sector. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address the following critical CIP challenges that we have identified:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing, which clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information-sharing relationships within the federal government and between the federal government and state and local governments and the private-sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private-sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government.

ISAC Structures and Operations Reflect Sector Needs and Evolving Goals

PDD 63 encouraged the voluntary creation of ISACs and suggested some possible activities, as discussed earlier; however, their actual design and functions were left to the private-sector, along with their relationship with the federal government. HSPD-7 continues to encourage the development of information-sharing mechanisms and does not suggest specific ISAC activities. As a result, the ISACs have been designed to perform their missions based on the unique characteristics and needs of their individual sectors and, although their overall missions are similar, they have different characteristics. They were created to provide an information-sharing and analysis capability for members of their respective infrastructure sectors to support efforts to mitigate risk and provide effective response to adverse events, including cyber, physical, and natural events. In addition,

the ISACs have taken several steps to improve their capabilities and the services they provide to their respective sectors.

Management and Operational Structures Vary, But Provide Similar Basic Capabilities

The ISACs have developed diverse management structures and operations to meet the requirements of their respective critical infrastructure sectors. To fulfill their missions, they have been established using various business models, diverse funding mechanisms, and multiple communication methods.

Business model—ISACs use different business models to accomplish their missions. Most are managed or operated as private entities, including the Financial Services, Chemical, Electricity Sector, Food, Information Technology, Public Transit, Real Estate, Surface Transportation, Highway, and Water ISACs. Many are established as part of an association that represents a segment of or an entire critical infrastructure sector. For example, the Association of Metropolitan Water Authorities manages the contract for the Water ISAC and the American Chemistry Council manages and operates the Chemical ISAC through its CHEMTRAC.[3] In addition, the North American Electric Reliability Council (NERC),[4] a nonprofit corporation that promotes electric system reliability and security, operates the Electricity Sector ISAC using internal expertise.

The legal structure of ISACs continues to evolve. The Financial Services ISAC has evolved from a limited liability corporation in 1999 to a 501(c)6 non-stock corporation and is managed by a board of directors that is comprised of representatives from the Financial Services ISAC's members. According to the Financial Services ISAC Board, the change to be a 501(c)6 non-stock corporation, as mentioned above, was made to simplify the membership agreement and to make the process for obtaining public funding easier. The Energy ISAC also changed from a limited liability corporation to a 501(c)3 nonprofit charitable organization to eliminate membership barriers.

[3]The American Chemistry Council represents the leading companies engaged in the business of chemistry. CHEMTREC® (Chemical Transportation Emergency Center) is the American Chemistry Council's 24-hour emergency communications center. It was established in 1971 to provide emergency responders technical assistance in safely mitigating a distribution incident.

[4]The North American Electric Reliability Council's (NERC) membership includes small and large electric utilities, regional utility companies, power marketers, and other entities responsible for power generation, transmission, control, and marketing and distribution in the United States, Canada, and a portion of Mexico.

Also, government agencies have partnered with the private-sector to operate certain ISACs. For example, DHS's National Communications Systems/ National Coordinating Center (NCC) for Telecommunications sponsors the Telecommunications ISAC, which is a government/industry operational and collaborative body.[5] DHS provides for the Telecommunications ISAC facilities, tools and systems, the NCC manager, and the 24x7 watch operations staff. The private-sector provides representatives who have access to key corporate personnel and other resources. In addition, DHS's United States Fire Administration operates the Emergency Management and Response ISAC. New York State, through its Office of Cyber Security and Critical Infrastructure Coordination, is coordinating efforts of the Multi-state ISAC. The New York State Office of Cyber Security and Critical Infrastructure Coordination is currently studying best practices and lessons learned to assist in developing a structure that will include representation by member states.

Six of the ISACs included in our study use contractors to perform their day-to-day operations. According to an Association of Metropolitan Water Agencies (AMWA) official, they chose a contractor to operate the Water ISAC because the contractor had the appropriate expertise. In addition, the contractor's personnel had government clearances and the ability to operate a secure communication system and facility. In addition, ISACs use contractors to supplement their operations. For example, a formal contract provides for the daily staffing and performance of the Emergency Management and Response ISAC's tasks. It chose this model because of federal requirements and the shortage of positions for federal full-time employees at the United States Fire Administration. The Telecommunications ISAC contracted for analysts to operate the 24 x 7 watch operations under the management of a government official.

ISACs also differ in the nature of the hazards that they consider: cyber, physical, or all hazards (including natural events such as hurricanes). For example, during events of the power outage in August 2003 and Hurricane

[5]The National Coordinating Center for Telecommunications is open to companies that provide telecommunications or network services, equipment, or software to the communications and information sector; select, competitive local exchange carriers; Internet service providers; vendors; software providers; telecommunications professional organizations and associations; or companies with participation or presence in the communications and information sector. Membership is also allowed for National Coordinating Center member federal departments and agencies, and for national security/emergency preparedness users.

Isabel in September 2003, the Financial Services ISAC was contacted by DHS to determine the Banking and Finance sector's preparedness and the impact of those events. However, the Multi-state ISAC will remain focused on cyber threats because other state organizations are in place to address physical and natural disaster events.

Funding— ISACs fund their activities using a variety of methods—fees-for-service, association sponsorship, federal grants, and voluntary, or in-kind, operations by existing participants. For example, the Financial Services, Information Technology, and Water ISACs use a tiered fee-for-service model for members. This model establishes different tiers of membership based on the level of service provided. These tiers typically include some basic level of service that is provided at minimal or no cost to the member and additional tiers that provide—for a fee—more personalized service and access to additional resources. To help ensure that cost is not a deterrent to membership and that the ISAC's coverage of its sector is extensive, the Financial Services ISAC recently, as part of its next-generation ISAC effort, shifted to a tiered fee-for-service approach. It offers five levels of service that vary in cost—Basic (no charge), Core ($750 per year), Premier ($10,000 per year), Gold ($25,000 per year), and Platinum ($50,000)—for ascending levels of information and analytical capabilities. In addition, there is a partner-level license agreement for select industry associations ($10,000) for distribution to eligible association members of Urgent and Crisis Alerts. For example, the Information Technology ISAC recently started to work on a tiered basis with fees set annually at $40,000; $25,000; $5,000; $1,000; and free. The Water ISAC also uses a tiered approach, with membership fees ranging from $7,500 to $750 annually. The Surface Transportation ISAC assesses an annual fee from its Class I railroad members of approximately $7,500.

Some industry associations that operate ISACs fund them from budgets. For example, the North American Electric Reliability Council (NERC) funds the Electricity Sector ISAC, and the American Trucking Association funds the Highway ISAC from their budgets. The American Chemistry Council fully funds the Chemical ISAC through the previously existing Chemical Transportation Emergency Center, known as CHEMTRAC. The ten trade associations that are members of it fund the Real Estate ISAC.

In addition, some ISACs receive funding from the federal government for such purposes as helping to start operations, funding memberships, and providing expanded capabilities. Examples include the following:

- The Public Transit ISAC initially received a $1.2 million grant from the Federal Transit Administration (FTA) to begin operations. Members pay

no an annual fee and there are no membership requirements from the association that started the ISAC—the American Public Transportation Association.

- For FY 2004, the Water ISAC received a $2 million grant from EPA to cover annual operating costs, including the expansion of memberships to smaller utilities.

- The Financial Services ISAC received $2 million dollars from the Department of the Treasury to enhance its capabilities, including technology to broaden membership service.

- The Highway ISAC received initial funding from DHS's Transportation Security Administration (TSA) to start the ISAC.

- The Energy ISAC received federal grants to assist entities within its separate sectors to be members.

- DHS provides funding for the operation of the Telecommunications ISAC that is combined with in-kind services provided by the corporate participants. DHS also fully operates the Emergency Management and Response ISAC.

States also provide funding for ISACs. For example, the Multi-state ISAC is funded by and functions as part of the New York State Cyber Security Analysis Center. In addition, the Research and Education Network ISAC is supported by Indiana University.

Sharing mechanisms—ISACs use various methods to share information with their members, other ISACs, and the federal government. For example, they generally provide their members access to electronic information via e-mail and Web sites. For example, the Chemical ISAC members receive e-mail alerts and warnings in addition to the information that is posted to the ISAC's Web site. The Highway ISAC provides members on its Web site with links to IT resources.

Some ISACs also provide secure members-only access to information on their Web sites. For example, the Financial Services ISAC's Web site offers multiple capabilities for members at the premier level and above, including, among other things, access news, white papers, best practices, and contacts. The Energy ISAC offers its members access to a secure Web site.

In addition, some ISACs hold conference calls for their members. For example, the Chemical ISAC holds biweekly conference calls with DHS. The Financial Services ISAC also conducts threat intelligence conference calls every two weeks for premier members and above with input from Science Applications International Corporation (SAIC) and DHS. These calls discuss physical and cyber threats, vulnerabilities and incidents that have occurred during the previous two weeks, and they provide suggestions on what may be coming. The Financial Services ISAC is capable of organizing crisis conference calls within an hour of the notification of a Crisis Alert, and it hosts regular bi-weekly threat conference calls for remediation of vulnerabilities (viruses, patches).

ISACs also use other methods to communicate. For example, they may use pagers, phone calls, and faxes to disseminate information. In addition, the Telecommunications ISAC uses the Critical Infrastructure Warning Information Network (CWIN).[6] The Financial Services ISAC also sponsors twice yearly members' only conferences to learn and share information.

ISAC Coverage and Participation Varies

According to the ISAC Council, its membership possesses an outreach and connectivity capability to approximately 65 percent of the U.S. private critical infrastructure. However, the ISACs use various matrices to define their respective sectors' participation in their activities. For example, the Banking and Finance sector has estimated that there are more than 25,000 financial services firms in the United States. Of those, according to the Financial Services ISAC Board, roughly 33 percent receive Urgent and Crisis Alerts through license agreements with sector associations—accounting for the vast majority of total commercial bank assets, the majority of assets under management, and the majority of securities/investment bank transactions that are handled by the sector, but less than half the sector's insurance assets. According to an American Public Transportation Association official, the Public Transit ISAC covers a little less than 5 percent of the public transit agencies; however, those agencies handle about 60 to 70 percent of the total public transit ridership. Further, according to NERC officials, virtually all members of NERC are members of the Electricity Sector ISAC. As for the Energy ISAC, officials stated that its 80-plus members represent approximately 85 percent of the energy industry. Membership in the Information Technology ISAC also represents 85 to 90 percent of the industry, including assets of Internet equipment

[6]CWIN provides connectivity and 24x7 alert and notification capability to government and industry participants. It is engineered to provide a reliable and survivable network capability, and it has no logical dependency on the Internet or the Public Switched Network.

hardware, software, and security providers. For other ISACs, such as Chemical and Real Estate, officials stated that it is difficult to determine the percentage of the sector that is included.

Table 2 provides a summary of the characteristics of the ISACs that we included in our review. In addition to these ISACs, the Healthcare sector is continuing to organize, including efforts to establish an ISAC. According to DHS officials, the Emergency Law Enforcement ISAC that was formally operated by the NIPC and transferred to IAIP is not currently staffed and will be considered in current efforts to organize the Emergency Services sector.

Table 2: Summary of ISAC Characteristics

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
Agriculture					
None at this time.					
Banking & Finance					
Financial Services (est. Oct. 1999)	200 members, including commercial banks, securities firms, and insurance companies. Represents 90% of the financial sector's assets.	Funded by and operated with tiered membership fees. Contractor operated.	Cyber Physical	Operates 24 hours a day, 7 days a week. Watch desk analyzes and categorizes threats, incidents, and warnings based on the sector's needs.	Text-based alerts, through a notification system, backed up by telephone. Biweekly threat intelligence conference call with DHS and SAIC.
Chemicals & Hazardous Materials					
Chemical (est. April 2002)	538 individual members representing the chemical industries. 285 businesses. Represents 90% of chemical sector.	Funded and operated by ACC's Chemical Transportation Emergency Center.	Cyber Physical	Operates 24x7. Currently working to develop an analysis center.	E-mails alerts and warnings. Chemistry ISAC Web site. Biweekly conference calls with DHS. Secure communications network with DHS.
Defense Industrial Base					
None at this time.					
Emergency Services					
Emergency Management & Response (est. Oct. 2000**)**	10 FEMA Regions 6 major stakeholders of EMR sector. Represents 100% of the essential	Funded by FEMA's Office of Cyber Security with supplementation from USFA. Contractor operated.	Cyber Physical	Developing 24x7 operations. Analyzes and disseminates actionable intelligence on threats,	Electronic messaging Telephone and when necessary, a secure telephone unit.

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
	components of the EMR Sector.			attacks, vulnerabilities, anomalies, and security best practices.	
Energy					
Electric (est. Oct. 2000)	More then 90% of NERC members are members of the ISAC including large and small electric utilities, regional electric utility companies, and power marketers.	Funded and managed/operated by NERC.	Cyber Physical	Operates 24x7. The ES-ISAC and NERC have created the Indications, Analysis, and Warnings Program (IAW) that provides a set of guidelines for reporting operational and cyber incidents that adversely affect the electric power infrastructure.	Secure telephone, fax, and Web server E-mail Satellite telephones. Information such as incident reports and warnings, vulnerability assessments, and related documents are posted on the public Web site.
Energy (est. Nov. 2001)	80 plus members from the oil and gas sector. Represents 85% of the oil and gas sector.	Funded by grants from DOE. Contractor operated.	Cyber Physical	Operates 24x7. Analyzes threats, vulnerabilities, and incident information. Provides security information and solutions.	Conference calls Fax, Email, pager. Detailed information on warnings provided on a membership only, secure Web site.
Food					
Food (est. Feb. 2002)	Over 40 food-industry trade associations and their members.	No current funding. Operated by volunteer labor from each member association.	Physical	Operates 24x7. No analysis capability, due to members' privacy concerns. Depends on DHS for analysis.	E-mail Watch Commander List Currently working to develop a secure e-mail system.
Government					
State Gov. (est. Jan. 2003)	49 states (excluding Kansas) and the District of Columbia.	Funded and operated by New York State. States provide time and resources as appropriate.	Cyber Physical & Natural (as it relates to cyber).	Operates 24x7. Issues bulletins, advisories, and alerts.	Monthly conference calls E-mail Telephone

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
Information Technology & Telecommunications					
IT (est. Dec. 2000)	90% of all desktop operating systems. 85% of all databases. 50% of all desktop computers. 85% of all routers. 65% of software security.	Funded and operated by foundational member contributions, will soon implement membership fees (tiered). Contractor operated.	Cyber Physical	Operates 24x7. Analyzes cyber alerts and advisories and reports physical issues.	CWIN Encrypted e-mail SSL-protected Web sites Cellular phones VoIP telephony GETS[7] system for priority calls
Telecom (est. Jan. 2000)	95% of wireline providers. Over 60% of wireline vendors. 95% of wireless providers. 90% of wireless vendors. 42% of Internet Service subscribers. 90% of Internet Service networks. 6 of the top system integrators in the U.S. Federal IT market. 15% of Domain Name Service root and global Top Level Domain operators.	Funded by NCS. Operated by NCC. Agencies bear the costs of their own personnel.	Cyber Physical Natural	Operates 24x7. Analyzes data to avoid crises that could affect the entire telecom infrastructure.	E-mail Telephone Fax Meetings CWIN
Research & Education Network (est. Feb. 2003)	200 Universities. All U.S. universities and colleges that are connected to national R&E networks have basic membership.	Funded and operated by Indiana University.	Cyber	Operates 24x7. Receives and disseminates information regarding network security vulnerabilities and threats in the higher education community.	Public information restricted to aggregate views of the network. Information identifying institutions or individuals not reported publicly. Detailed and sensitive information shared only with affected institutions.

[7]Government Emergency Telecommunications Service (GETS)

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
Postal & Shipping					
None at this time.					
Public Health & Healthcare					
HealthCare					
None at this time.					
Transportation					
Public Transit (est. Jan. 2003)	Approximately 100 of the major national transit organizations.	Federally funded. Contractor operated.	Cyber Physical	Operations 24x7. Collects, analyzes, and disseminates security information.	E-mail tree Secure e-mail Public Transit Web site Links to HSOC, and DOT and TSA's Operation Centers.
Surface Transportation (est. May 2002)	Includes the major North American freight railroads and Amtrak. Represents 95% of the U.S. freight railroad industry and Amtrak.	Funded by membership fees and a grant from the Federal Transit Administration (FTA). Contractor operated.	Cyber Physical Natural	Operates 24x7. Conducts mid- to long-term technical analysis on all threats.	Surface Transportation Web site. Secure telephone.
Highway (est. March 2003)	Over 90% of the largest for-hire motor carriers. Represents 60% economic activity with over 50% of long haul.	Funded and operated by the American Trucking Association (ATA).	Cyber Physical	Developing 24x7 operations. Channels warnings, threat information, and advisories to the industry and to drivers through its call center.	Highway ISAC Web site Highway watch center Blast fax E-mail Print media communications Amber alerts
Drinking Water & Water Treatment Systems					
Water (est. Dec. 2002)	275-300 small and large water utilities. Represents 45% of water utilities with secure portals. Represents 85% of the water utilities that receive e-mail alerts.	Funded by tired membership fees and a grant from EPA. Contractor operated. Receives contributions from AMWA.	Cyber Physical	Operates 24x7. Analyzes threat and incident information for its potential impact on the sector.	Encrypted e-mail Secure portal Secure electronic bulletin boards and chat rooms

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
Other Sectors That Have Established ISACs					
Real Estate (est. April 2003)	10 trade associations representing hotels, realtors, shopping centers, and others.	Funded by trade associations. Contractor operated.	Physical	Operates 24x7. Depends on DHS for threat analysis.	2-way communications network and Web site Conference calls with top executives from various sectors as needed.

Sector Coordinator Roles Differ

As discussed earlier, federal CIP policy establishes the position of sector coordinator for identified critical infrastructure sectors to initiate and build cooperative relationships across an entire infrastructure sector. In most cases, sector coordinators have played an important role in the development of their respective infrastructure sectors' ISACs. In many cases the sector coordinator also manages or operates the ISAC.

- The North American Electric Reliability Council, as sector coordinator for the electricity segment of the energy sector, operates the Electricity Sector ISAC.
- The Association of American Railroads, as a sector coordinator for the transportation sector, manages the Surface Transportation ISAC.
- The Association of Metropolitan Water Agencies, as the sector coordinator for the water and wastewater sector, manages the Water ISAC.

In addition, regarding the telecommunications ISAC, sector coordinators participate as members of the ISAC. For example, the Cellular Telecommunications and Internet Association, the United States Telecom Association, and the Telecommunications Industry Association are all members of the NCC, which operates the telecommunications ISAC. In the case of the Financial Services ISAC, no formal relationship exists between the Banking and Finance Sector Coordinator, the Financial Services Sector Coordinating Council, and the ISAC; however, according to Financial Services ISAC officials, there is a good relationship between them.

Other ISACs were created and are operated without a formal sector coordinator in place, including the Chemical, Emergency Management and Response, and Food ISACs.

Council Established to Improve ISACs' Efficiency and Effectiveness

Eleven ISACs created an ISAC Council to work on various operational, process, and other common issues to effectively analyze and disseminate information and, where possible, to leverage the work of the entire ISAC community. The ISACs initiated this effort without federal sponsorship. Currently, the participating ISACs include Chemical, Electricity, Energy, Financial Services, Information Technology, Public Transit, Surface Transportation, Telecommunications, Highway, and Water. In addition, the Multi-state and Research and Education Networks ISACs are participants.

In February 2004, the council issued eight white papers to reflect the collective analysis of its members and to cover a broad set of issues and challenges, including

- **Government/Private-sector Relations**. Explains the need for DHS to clarify its expectations and to develop roles and responsibilities for the ISACs.
- **HSPD-7 Issues and Metrics**. Describes specific issues related to the private-sector that DHS should address when responding to HSPD-7.
- **Information Sharing and Analysis**. Identifies future goals that the ISACs may want to work on achieving, including developing an implementation plan.
- **Integration of ISACs into Exercises**. Discusses the importance of the ISACs and the private infrastructure sectors being involved in government exercises that demonstrate responses to possible incidents.
- **ISAC Analytical Efforts**. Describes the various levels of capabilities that individual ISACs may want to consider supporting, including cyber and physical analysis.
- **Policy and Framework for the ISAC Community**. Identifies common policy areas that need to be addressed to provide effective, efficient, and scalable information sharing among ISACs and between ISACs and the federal government.
- **Reach of Major ISACs**. Describes and identifies the degree of outreach that the ISACs have achieved into the U.S. economy. As of September 2003, the ISAC Council estimated that the ISACs had reached approximately 65 percent of the critical infrastructures they represent.

- **Vetting and Trust**. Discusses the processes for sharing information and the need to develop trust relationships among individual ISAC members and among the various ISACs.

Federal Efforts to Establish Cooperation and Interaction with the ISACs Continue

As outlined in HSPD-7 and presented in table 1, DHS and other federal agencies are designated as sector-specific agencies for the critical infrastructure sectors identified. In addition, DHS is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States and has established organizational structures to address its CIP and information-sharing responsibilities. DHS and the sector-specific agencies have undertaken a number of efforts to address the public/private partnership that is called for by federal CIP policy, and they continue to work on their cooperation and interaction with the ISACs and with each other.

DHS Actions to Improve Information-sharing Relationships

The functions DHS provides to each ISAC differ, and its coordination and levels of participation vary for each sector-specific agency. However, the department has undertaken a number of efforts with the ISACs and sector-specific agencies to implement the public/private partnership called for by federal CIP policy.

DHS has established functions within the department to support the ISACs and other CIP efforts. IAIP, as the DHS component directly responsible for CIP activities, carries out many of these functions. The Infrastructure Coordination Division within IAIP plays a key role in coordinating with the ISACs concerning information sharing. Nonetheless, ISACs may interact with multiple components of the department. For example, the ISACs may discuss cyber issues with the National Cyber Security Division. According to a DHS official, the department does not intend to establish a single point of contact for ISACs within the department. Rather, the department plans to develop policies and procedures to ensure effective coordination and sharing of ISAC contact information among the appropriate DHS components. In addition, the Infrastructure Coordination Division is in the process of staffing analysts who are responsible for working with each critical infrastructure sector. The analysts would serve as the primary point of contact for the sectors and would address information sharing, coordination, information protection, and other issues raised by the sectors.

Further, according to DHS officials, TSA, within the department's Border and Transportation Security Directorate, is working with organizations in the private sector to establish information-sharing relationships. For example, Surface Transportation ISAC analysts stated that they have a

good working relationship with TSA, and TSA's Operations Center has office space designated for them.

In addition, other DHS actions include the following:

- Last summer, DHS, the Department of Agriculture (USDA), and the Department of Health and Human Services' (HHS) Food and Drug Administration (FDA) initiated efforts to organize the agriculture and food critical infrastructure sectors to raise awareness and improve security efforts. An introductory conference was held with about 100 leading sector corporations and associations to make the business case for participating in CIP efforts, including the importance of enhancing security and sharing information within the sectors.

- In December, DHS hosted a 2-day CIP retreat with ISAC representatives, sector coordinators, and high-level DHS and White House Homeland Security Council officials. Participants discussed the needs, roles, and responsibilities of public- and private-sector entities related to information sharing and analysis, incident coordination and response activities, critical infrastructure information requests, and level of DHS funding. During this retreat, DHS participated in the first meeting of the Operational Clarity and Improvement Task Group, which was formed by the ISAC Council and sector coordinators to address the need for a common conceptual framework and to clarify current and future efforts to protect the nation's critical infrastructure.

- In January, DHS's IAIP Directorate held a 2-day conference to describe the information it is analyzing and the use of that information in the partnership with the private sector to discuss information sharing between the federal government and the private sector.

- In February, the department established the Protected Critical Infrastructure Information (PCII) Program, which enables the private sector to voluntarily submit infrastructure information to the government. DHS's IAIP Directorate is responsible for receiving submissions, determining if the information qualifies for protection and, if it is validated, sharing it with authorized entities for use as specified in the Critical Infrastructure Information Act of 2002.

In addition to the efforts listed above, DHS officials stated that they provide funding to some of the ISACs. For example, DHS has agreed to fund tabletop exercises for the Financial Services, Telecommunications, and Electricity Sector ISACs. DHS anticipates that the tabletop exercises will be completed by August 2004. Also, DHS expects to fund a cross-

sector tabletop exercise. According to the Financial Services ISAC, funding for their tabletop exercise is $250,000.

Another effort that DHS has undertaken is to maintain regular contact with the ISACs. For example, a DHS analyst specializing in the chemical sector stated that the Chemical ISAC is in daily contact with DHS and that it participates in DHS-sponsored biweekly threat meetings. The department also conducts weekly conference calls with several ISACs, other DHS components, and private-sector organizations to discuss threats and viruses.

Sector-specific Agencies Have Taken Action to Assist the ISACs

HSPD-7 designates federal departments and agencies to be sector-specific agencies. These federal agencies, among other things, are to collaborate with the private sector and continue to encourage the development of information-sharing and analysis mechanisms. In addition, sector-specific agencies are to facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Another directive, HSPD-9, establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. Some sector-specific agencies have taken steps to help the ISACs to increase their memberships and breadth of impact within their respective sectors and to improve their analytical and communications capabilities.

- **Environmental Protection Agency (EPA)**. As noted earlier, EPA is the sector-specific agency for the water sector. According to EPA officials, its Office of Water (Water Security Division), which has been designated as the lead for drinking water and wastewater CIP efforts, is currently revising EPA's Office of Homeland Security's Strategic Plan. In addition, the division is working on a General Strategic Plan, to identify measurable goals and objectives and determine how the division will accomplish that work. Further, these officials stated that for fiscal year 2004, EPA issued a $2 million grant to the Water ISAC to enhance its capabilities, for example, to fund 24x7 operations and to increase and support ISAC membership. They also stated that EPA issued $50 million in grants to assist the largest drinking water utilities in conducting vulnerability assessments. There are also state grants to build communications networks for disseminating information, particularly to smaller utility companies. EPA's Water Security Division also makes publicly available various resources related to water security including, among other things, emergency response guidelines, risk assessment and vulnerability assessment methodologies, and a security product guide. The division has also developed a "Vulnerability Assessment Factsheet" that gives utility

companies additional guidance on vulnerability assessments. Moreover, the Water Security Division holds biweekly conference calls with water associations to promote communications between EPA and the private sector, and it provides EPA publications and other information to the Water ISAC through e-mail distribution lists. In addition, the division has 10 regional offices that work with the states.

- **Department of the Treasury (Treasury)**. As the sector-specific agency for the Banking and Finance sector, Treasury's Office of CIP and Compliance Policy is responsible for CIP-related efforts. It has developed policy for its role as a sector-specific agency. The policy includes steps to identify vulnerabilities with the assistance of the institutions, identify actions for remediation, and evaluate progress in reducing vulnerabilities. A major effort by Treasury was having consultants work with the Financial Services ISAC's board of directors to evaluate ways to improve the overall reach and operations of the ISAC. According to Treasury officials, this effort, in part, led to a $2 million grant from Treasury to the ISAC for developing the "next generation" Financial Services ISAC. The one-time grant was earmarked for enhancing the ISAC's capabilities. Regarding interaction with the Financial Services ISAC, Treasury informally shares high-level threat and incident information with the sector through the ISAC. The department also chairs the Financial and Banking Information Infrastructure Committee (FBIIC), a group of regulators who coordinate regulatory efforts to improve the reliability and security of financial systems. This group has done a number of things to raise awareness and improve the reliability of the institutions. For example, under the sponsorship of the Federal Deposit Insurance Corporation, there are regional outreach briefings that address why the private sector needs to partner with the federal government to improve its security. Moreover, FBIIC has sponsored the 3,600 priority telecommunications circuits for financial institutions under the National Communications System's Telecommunications Service Priority and Government Emergency Telecommunications Service programs.

- **Department of Energy (DOE)**. As the sector-specific agency for the Energy and Electricity sectors, DOE's Office of Energy Assurance is responsible for fulfilling the roles of critical infrastructure identification, prioritization, and protection for the energy sector, which includes the production, refining, and distribution of oil and gas, and electric power—except for commercial nuclear power facilities. However, DOE does not address situational threats such as natural disasters or power outages with its ISACs because, in part, the ISACs

are determining whether it is their role to address these types of threats. Information sharing with the ISACs is an informal process, and no written policy exists. For example, DOE is collecting threat information related to hackers and computer security, but the department is not disseminating it to the ISACs or to private industry. The Office of Energy Assurance hopes to clarify and expand on this subject in its International Program Plan, which is currently in draft form.

- **Department of Health and Human Services (HHS)**. As mentioned earlier, HHS is the sector-specific agency for the public health and healthcare sector, and it shares that role with USDA for the food sector. Currently, there is no ISAC for the healthcare sector. Efforts to organize the healthcare sector have been ongoing. In July 2002, HHS officials and other government and industry participants were invited to the White House conference center to discuss how they wanted to organize the sector. A Healthcare Sector Coordinating Council (HSCC) was formed, and HHS requested that MITRE, its contractor, lend technical support to the new group as it continues to organize the sector and establish an ISAC. In addition, HHS officials stated that the department provided $500,000 for ISAC efforts in fiscal year 2003 and budgeted $1 million for fiscal year 2004. HHS officials stated that the department would likely be agreeable to continuing to provide funding for an ISAC. They also stated that an ISAC could be operational within the next year. In the meantime, HHS is sharing information with the industry through an e-Community group that MITRE has set up on a secure Web site.

  Agriculture and Food were only recently designated as critical infrastructure sectors and, as with the healthcare sector, efforts to organize the sectors are in the beginning stages. HHS has worked with the Food Marketing Institute-operated Food ISAC since it was established, but the department has focused more of its efforts on organizing the agriculture and food sectors. As we mentioned earlier, HHS helped initiate efforts to organize the sector by holding an introductory conference last summer for about 100 leading sector corporations and associations to make the business case for participating in CIP efforts. Recently, the department co-hosted a meeting with DHS and USDA in which industry participants were asked how they wished to organize into an infrastructure sector, including addressing the existence and expansion of the current Food ISAC. As a result of this meeting, participants agreed to establish a council of about 10-15 private-sector food and agriculture organizations to represent the sector. A federal government council

will be created to interact with the private sector and with state and local governments. The government council will initially include several federal government agencies and state and local entities. According to HHS officials, the timeframe for organizing the sector and setting up an expanded Food ISAC has not been determined, but officials anticipated this occurring by fall of 2004.

- **Department of Agriculture (USDA)**. As mentioned above, USDA shares with HHS the sector-specific agency designation for the food sector. USDA participated in a conference held last summer and a recent meeting with the industry. In addition to those events, USDA's Homeland Security Council Working Group is involved in enhancing the agriculture sector's information-sharing and analysis efforts, which may include replacing or improving the current Food ISAC. Another USDA effort uses training to reach out to the industry and raise awareness. For example, USDA is providing training to private-sector veterinarians and animal hospitals on recognizing possible signs of bioterrorism activity.

Although no longer a sector-specific agency for the transportation sector, DOT, through its Federal Transit Administration, has provided a grant to the Public Transportation ISAC to provide for memberships at no cost.

Challenges to ISAC Establishment and Partnership with the Federal Government

Our discussions with the ISACs and the series of ISAC Council white papers confirmed that a number of challenges remain to the successful establishment and operation of ISACs and their partnership with DHS and other federal agencies. Highlighted below are some of the more significant challenges identified, along with any successful ISAC practices and related actions that have been taken or planned by DHS or others.

Increasing Sector Participation and Reach

Many of the ISACs report that they represent significant percentages of their industry sectors; at least one—the Electricity ISAC—reports participation approaching 100 percent. The ISAC Council estimates that the overall ISAC community possess an outreach and connectivity capability to reach approximately 65 percent of the private critical infrastructure. The Council also recognizes the challenge of increasing sector participation, particularly to reach smaller entities that need security support, but have insufficient resources to actively contribute and pay for such support. Officials in DHS's IAIP acknowledge the importance of reaching out to critical infrastructure entities, and are considering alternatives to address this issue.

The Financial Services ISAC provides a notable example of efforts to respond to this challenge. Specifically, officials for this organization

reported that, as of March 2003, its members represented a large portion of the sector's assets, but only 0.2 percent of the number of entities with small financial services firms and insurance companies, in particular, were underrepresented. To increase its industry membership, this organization established its next generation ISAC, which provides different levels of service—ranging from a free level of basic service to fees for value-added services—to help ensure that no entity is excluded because of cost. Further, it has set goals of delivering urgent and crisis alerts to 80 percent of the Banking and Finance sector by the end of 2004 and to 99 percent of the sector by the end of 2005. To help achieve these goals, the Financial Services ISAC has several other initiatives under way, including obtaining the commitment of the Financial Services Sector Coordinating Council (FSSCC—the sector coordinator and primary marketing arm for this ISAC) to drive the marketing campaign to sign up its members for the appropriate tier of service; encourage membership through outreach programs sponsored by the Federal Deposit Insurance Corporation and the FSSCC in 24 cities; and to work with individual sector regulators to include in their audit checklists whether a firm is a member of the ISAC. The Financial Services ISAC believes that its goals are attainable and points to its industry coverage, which it says had already increased to 30 percent in March 2004—only three months after its new membership approach began in December 2003.

Other issues identified that were related to increasing sector participation and reach included the following,

- Officials at two of the ISACs we contacted considered it important that the federal government voice its support for the ISACs as the principal tool for communicating threats.

- The ISAC Council has suggested that a General Business ISAC may need to be established to provide baseline security information to those general businesses that are not currently supported by an ISAC.

- Many of the industries that comprise our nation's critical infrastructures are international in scope. Events that happen to a private infrastructure or public sector organization in another country can have a direct effect in the United States, just as events here could have effects in other countries. Therefore, an ISAC may need to increase its reach to include the reporting and trust of international companies and organizations.

Building Trusted Relationships

A key element in both establishing an ISAC and developing an effective public/private partnership for CIP is to build trusted relationships and processes. From the ISAC perspective, sharing information requires a

trusted relationship between the ISAC and its membership, such that companies and organizations know their sensitive data is protected from others, including competitors and regulatory agencies. According to the ISAC Council, the ISACs believe that they provide a trusted information-sharing and analysis mechanism for private industry in that they manage, scrutinize, establish, and authenticate the identity and ensure the security of their membership, as well as ensuring the security of their own data and processes. Other steps taken by ISACs to safeguard private companies' information, which may help to foster trusted relationships, included sharing information with other entities only when given permission to do so by the reporting entity and providing other protections, such as distributing sensitive information to subscribers through encrypted e-mail and a secure Web portal.

Building trusted relationships between government agencies and the ISACs is also important to facilitating information sharing. In some cases, establishing such relationships may be difficult because sector-specific agencies may also have a regulatory role; for example, the Environmental Protection Agency has such a role for the Water sector and HHS' Food and Drug Administration has it for portions of the Food and Agriculture sectors.

Information Sharing Between the Private Sector and Government

Sharing information between the federal government and the private sector on incidents, threats, and vulnerabilities continues to be a challenge. As we reported last year, much of the reluctance by ISACs to share information has focused on concerns over potential government release of that information under the Freedom of Information Act, antitrust issues resulting from information sharing within an industry, and liability for the entity that discloses the information.[8] However, our recent discussions with the ISACs—as well as the consensus of the ISAC Council—identified additional factors that may affect information sharing by both the ISACs and the government.

The ISACs we contacted all described efforts to work with their sector-specific agencies, as well as with other federal agencies, ISACs, and organizations. For example, the Public Transit ISAC said that it provides a critical link between the transit industry, DOT, TSA, DHS, and other ISACs for critical infrastructures and that it collects, analyzes, and distributes

[8]U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* GAO-03-173 (Washington, D.C.: Jan. 30, 2003); and *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors,* GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

cyber and physical threat information from a variety of sources, including law enforcement, government operations centers, the intelligence community, the U.S. military, academia, IT vendors, the International Computer Emergency Response Community, and others. Most ISACs reported that they believed they were providing appropriate information to the government but, while noting improvements, still had concerns with the information being provided to them by DHS and/or their sector-specific agencies. These concerns included the limited quantity of information and the need for more specific, timely, and actionable information. In particular, one ISAC noted that it receives information from DHS simultaneously with or even after news reports, and that sometimes the news reports provide more details.

In its recent white papers, the ISAC Council also has identified a number of barriers to information sharing between the private sector and government. These included the sensitivity of the information (such as law enforcement information), legal limits on disclosure (such as Privacy Act limitations on disclosure of personally identifiable information), and contractual and business limits on how and when information is disclosed (e.g., the Financial Services ISAC does not allow any governmental or law enforcement access to its database). But the Council also emphasized that perhaps the greatest barriers to information sharing stem from practical and business considerations in that, although important, the benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable. Thus, to make information sharing real, it is essential to lower the practical risks of sharing information through both technical means and policies, and to develop internal systems that are capable of supporting operational requirements without interfering with core business. Consequently, the technical means used must be simple, inexpensive, secure, and easily built into business processes.

According to the Council, the policy framework must reduce perceived risks and build trust among participants. Further, the Council identified three general areas that must be addressed in policy for the information-sharing network to assure network participants that there is good reason to participate and that their information will be dealt with appropriately. These areas concern policies related to what information is shared within ISACs, across ISACs, and to and from government; actions to be performed at each node in the information-sharing network, including the kinds of analysis to be performed; and the protection of shared information and analysis in terms of both limitations on disclosure and use and information security controls.

The white papers also described the processes that are believed to be needed to ensure that critical infrastructure and/or security information is made available to the appropriate people with reasonable assurance that it cannot be used for malicious purposes or indiscriminately re-distributed so as to become essentially public information. These processes and other information-sharing considerations and tasks identified by the Council included the following:

- The ISAC information-sharing process needs to recognize two types of information categories—classified and sensitive but unclassified. However, the majority of information sharing must focus on the unclassified "actionable element" that points the recipient to a problem and to remediation action.

- Each ISAC is responsible for initially validating the trust relationship with its member organizations and for periodically re-assessing that trust relationship. The security structure must understand and continually be in dialogue with its vetted members and must manage this trusted relationship.

- Each individual who receives shared information must have a background check completed by and at a level of comprehensiveness specified by the sponsoring organization.

- Consequences and remediation must be developed and understood to address situations in which information is disclosed improperly—either intentionally or unintentionally.

- The government's data and information requirements for the sectors and the sectors' requirements for the government need to be defined.

- The government should establish a standing and formal trusted information-sharing and analysis process with the ISACs and sector coordinators as the trusted nodes for this dissemination. This body should be brought in at the beginning of any effort, and DHS products should be released to this group for primary and priority dissemination to their respective sectors.

Building this trusted information-sharing and analysis process is also dependent on the protections the government provides for the sensitive data shared by ISACs and private companies. As discussed earlier, DHS recently issued the interim rule for submitting protected critical infrastructure information, which provides restrictions on the use of this information and exempts it from release under the Freedom of

Information Act. However, it remains to be seen whether these protections will encourage greater private-sector trust and information sharing with the federal government.

Identifying Roles and Responsibilities

Federal CIP law and policies, including the Homeland Security Act of 2002, the *National Strategy to Secure Cyberspace*, and HSPD-7, establish CIP responsibilities for federal agencies, including DHS and others identified as sector-specific agencies for the critical infrastructure sectors. However, the ISACs believe that the roles of the various government and private-sector entities involved in protecting critical infrastructures must continue to be identified and defined. In particular, officials for several ISACs wanted a better definition of the role of DHS with respect to them. Further, officials for two ISACs thought other agencies might more appropriately be their sector-specific agencies. Specifically, the Energy ISAC would like its sector-specific agency to be DHS and not the Department of Energy, which is also the regulatory agency for this sector. On the other hand, the Highway ISAC thought its sector-specific agency should be the Department of Transportation—the regulatory agency for its sector—and not DHS.

The ISAC Council also identified the need for DHS to establish the goals of its directorates and the relationships of these directorates with the private sector. The Council also wants clarification of the roles of other federal agencies, state agencies, and other entities—such as the National Infrastructure Assurance Council.

Obtaining Government Funding

Ten of the ISACs we contacted, plus the Healthcare sector, emphasized the importance of government funding for purposes including creating the ISAC, supporting operations, increasing membership, developing metrics, and providing for additional capabilities. According to ISAC officials, some have already received federal funding: the Public Transit ISAC initially received a $1.2 million grant from the Federal Transit Administration to begin operations, and the Water ISAC received a $2 million grant from EPA for fiscal year 2004 to cover annual operating costs and expand memberships to smaller utilities. In addition, the Financial Services ISAC received $2 million from the Department of the Treasury to help establish its next-generation ISAC and its new capabilities, including adding information about physical threats to the cyber threat information it disseminates.

Despite such instances, funding continues to be an issue, even for those that have already received government funds. For example, the Healthcare Sector Coordinating Council, which is the sector coordinator for the healthcare industry, is currently looking to the federal government to help fund the creation of a Healthcare ISAC. Also, officials at the Public Transit

ISAC noted that funding is an ongoing issue that is being pursued with DHS. Officials at the Financial Services ISAC, who notes that the ISAC's goal is to become totally self-funded through membership fees by 2005, are also seeking additional government funding for other projects.

The ISAC Council has also suggested that baseline funding is needed to support core ISAC functionalities and analytical efforts within each sector. The Council's suggestions include that the government should procure a bulk license for the ISACs to receive data directly from some vulnerability and threat sources and access to analytical or modeling tools and that the funding for an ISAC analyst to work at DHS to support analysis of sector-specific information or intelligence requirements.

According to the Financial Services ISAC, DHS has agreed to fund tabletop exercises for some ISACs. For example, according to DHS officials, exercises are occurring this week involving the Banking and Finance sector and exercises for other sectors are currently being explored. In addition, energy sector-related exercises were held earlier in the year. DHS officials also stated that funding considerations for the critical infrastructure sectors and the ISACs would be based on their needs.

Utilizing Sector Expertise

In our discussions with ISAC officials, several, such as officials from the Surface Transportation and the Telecommunications ISACs, highlighted their analysis capabilities and, in particular, their analysts' sector-specific knowledge and expertise and ability to work with DHS and other federal agencies. The ISAC Council also emphasized that analysis by sector-specific, subject matter experts is a critical capability for the ISACs, intended to help identify and categorize threats and vulnerabilities and then identify emerging trends before they can affect critical infrastructures. Sector-specific analysis can add critical value to the information being disseminated, with products such as 24/7 immediate, sector-specific, physical, cyber, all threat and incident report warning; sector-specific information and intelligence requirements; forecasts of and mitigation strategies for emerging threats; and cross-sector interdependencies, vulnerabilities, and threats.

The Council also emphasized that although government analytical efforts are critical, private-sector analytical efforts should not be overlooked and must be integrated into the federal processes for a more complete understanding. The private sector understands its processes, assets, and operations best and can be relied upon to provide the required private-sector subject matter expertise.

In a few cases, the integration of private-sector analytical capabilities with DHS does occur. For example, the Telecommunications ISAC, as part of

DHS's National Communication System, has watch standers that are part of the DHS operations center and share information, when the information owner allows it and when it is appropriate and relevant, with the other analysts. In addition, a Surface Transportation ISAC analyst also participates in the DHS operations center on a part-time basis to offer expertise and connection to experts in the field in order to clarify the impact of possible threats.

Participation in National Homeland Security Exercises

The ISAC Council highlighted the need for ISAC participation in the national-level homeland security exercises that are conducted by the federal government, such as DHS's May 2003 national terrorism exercise (TOPOFF 2), which was designed to identify vulnerabilities in the nation's domestic incident management capability. However, according to the Council, there has been little or no integration of active private industry and infrastructure into such exercises. For example, private industry participation in TOPOFF 2 was simulated. The Council believes that with such participation, both national and private-sector goals could be established during the creation of the exercise and then addressed during the exercise.

The Council did identify examples where the private sector is being included in exercises, such as efforts by the Electronics Crime Unit of the U.S. Secret Service to reach out to the private sector and support tabletop exercises to address the security of private infrastructures. Further, according to a DHS official, the department has agreed to fund tabletop exercises for members of several ISACs, including Financial Services, Chemical, and Electricity, as well as a cross-sector tabletop exercise.

Additional Challenges

Additional challenges identified by our work and/or emphasized by the ISAC Council included the following.

- **Obtaining Security Clearances to Share Classified Information**. As we reported last year, several ISACs identified obtaining security clearances as a challenge to government information sharing with the ISACs. Seven of the 15 ISACs with which we discussed this issue indicated either that some of their security clearances were pending or that additional clearances would be needed.

- **Identifying Sector Interdependencies**. Federal CIP policy has emphasized the need to identify and understand interdependencies between infrastructure sectors. The ISAC Council also highlighted the importance of identifying interdependencies and emphasized that they require partnerships between the sectors and the government and could only be modeled, simulated, or "practiced" once the individual sectors'

dynamics are understood sufficiently. The current short-term focus for the ISACs is to review the work done by the government and the sectors regarding interdependencies. Similarly, a DHS official acknowledged the importance of identifying interdependencies, but that it is a longer-term issue.

- **Establishing Communications Networks**. Another issue raised through the ISAC Council's white papers was the need for a government-provided communications network for secure information sharing and analysis. Specifically, the Council suggested that although functionality would be needed to satisfy the ISAC s' requirements, DHS's Critical Infrastructure Warning Information Network (CWIN) could be used as an interim, first-phase communications capability. According to the Council, some of the ISACs are conducting routine communications checks at the analytical level in anticipation of expanded use of CWIN. In discussing this issue with a DHS official, he said that ISAC access to a secure communications network would be provided as part of the planned Homeland Security Data Network (HSDN). DHS recently announced a contract to initiate the implementation of HSDN, which is be a private, certified, and accredited network that provides DHS officials with a modern IT infrastructure for securely communicating classified information. According to DHS, this network will be designed to be scalable in order to respond to increasing demands for the secure transmission of classified information among government, industry, and academia to help defend against terrorist attacks.

DHS Information-Sharing Plan

At the time of our study, the relationship and interaction among DHS, the ISACs, sector coordinators, and other sector-specific agencies was still evolving, and DHS had not yet developed any documented policies or procedures. As we discussed earlier, HSPD-7 requires the Secretary of Homeland Security to establish uniform policies for integrating federal infrastructure protection and risk management activities within and across sectors. According to a DHS official, the department is developing a plan (referred to as a "roadmap") that documents the current information-sharing relationships among DHS, the ISACs, and other agencies; goals for improving that information-sharing relationship; and methods for measuring the progress in the improvement. According to this official, the plan is to define the roles and responsibilities of DHS, the ISACs, and other entities, including a potential overlap of ISAC-related responsibilities between IAIP and the Transportation Security Administration. Further, the official indicated that, in developing the plan, DHS would consider issues raised by the ISAC Council.

In summary, since first encouraged by federal CIP policy almost 6 years ago, private-sector ISACs have developed and evolved into an important facet of our nation's efforts to protect its critical infrastructures. They face challenges in increasing their sector representation and, for some, ensuring their long-term viability. But they have developed important trust relationships with and between their sectors—trust relationships that the federal government could take advantage of to help establish a strong public/private partnership. Federal agencies have provided assistance to help establish the ISACs, and more may be needed. However, at this time, the ISACs and other stakeholders, including sector-specific agencies and sector coordinators, would benefit from an overall strategy, as well as specific guidance, that clearly described their roles, responsibilities, relationships, and expectations. DHS is beginning to develop a strategy, and in doing so, it will be important to consider input from all stakeholders to help ensure that a comprehensive and trusted information-sharing process is established.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317 or Ben Ritt, Assistant Director, at (202) 512-6443. We can also be reached by e-mail at daceyr@gao.gov and rittw@gao.gov, respectively.

Other individuals making key contributions to this testimony included William Cook, Joanne Fiorino, Michael Gilmore, Barbarol James, Lori Martinez, and Kevin Secrest.

(310527)